APPENDIX 10: EVOLVING ROLES TO SUPPORT INFORMATION TECHNOLOGY FOR PUBLIC HEALTH

The new technologies that make information collection, processing, and exchange more efficient for public health agencies also require new staff responsibilities. The Information Technology Committee has identified the following roles and activities that must be present in every agency to keep information systems efficient and secure.

Technology roles for agency administration and management

- Assign roles for agency and clearly communicate expectations; provide guidance and guidelines.
- Develop a coordinated approach to approve individuals for access to specific applications and to approve the "rights" to be granted each individual for each application (i.e., types of rights, application administrators, supervisor access for monitoring program or employee performance, user-only, etc.). Decide who in the agency—among supervisors, managers, and program directors—will approve individuals for access to specific applications and who will communicate this information to the state Department of Health.
- Decide who will go to which trainings and how often.
- Decide and approve how much of which type of equipment to acquire.
- Decide and approve use policies— expectations, monitoring, and consequences regarding security, timeliness, accuracy, accountability, and acceptable behavior regarding use.

Technology roles that might be assigned to the IT manager

- Decide how much of which type of equipment to acquire.
- For individuals approved for access and specific rights to specific applications, arrange for necessary and appropriate equipment, security tools such as digital certificates, training, etc., and communicate this information to the state Department of Health.
- Maintain the list of who has access, and the specific rights granted, to which applications. Communicate this information, as appropriate, routinely to state Department of Health.
- Maintain a tracking system that includes 1) who has been granted access and which type of rights to what; 2) who has signed the necessary paperwork, such as security and confidentiality statements and data-sharing agreements; 3) who has been trained in what and who is due for training; 4) when each digital certificate expires or needs to be renewed, etc. Communicate this information, as appropriate, routinely to state Department of Health.
- Maintain current contact or profile information, such as accurate e-mail addresses for each user. Manage a reminder system to queue employees to update their own contact information and profile. Communicate this information, as appropriate, routinely to state Department of Health.
- Maintain a collection of current policies regarding data access and a current list of who may grant approval.

- Serve as information coordinator in assuring that once an employee has been appropriately approved for access to an application, the agency's application administrator or technical staff make the appropriate changes.
- Assign individuals to "administer" the application within the agency or region—i.e., with WaSECURES and LMS, local health jurisdictions will administer and manage their own use of the application. This will require significant training and frequent (sometimes daily) work with the application.
- Serve as main point of contact for the local health jurisdiction in communications with the state Department of Health application, program, or technical staff.
- Serve as the agency technical resource for the specific application.
- Provide general technical resource per agency policy.

Technology roles that might be assigned to human resources or quality improvement or assurance managers

- Develop a coordinated approach to approve individuals for access to specific applications and to approve the "rights" to be granted each individual for each application (i.e., types of rights, application administrators, supervisor access for monitoring program or employee performance, user-only, etc.). Decide who in the agency—among supervisors, managers, and program directors—will approve individuals for access to specific applications and who will communicate this information to the state Department of Health.

- Maintain current contact or profile information, such as accurate e-mail addresses for each user. Manage a reminder system to queue employees to update their own contact information and profile. Communicate this information, as appropriate, routinely to state Department of Health.
- Maintain collection of current policies regarding data access and a current list of who may grant approval.

Technology roles needed at the State Department of Health

- Establish a single point of contact to learn about each application—technical specifications, equipment and security requirements, user and administrator training, access help desk resources, types of rights available for users, etc.
- Establish a single point of contact for local health jurisdictions to arrange for necessary and appropriate equipment, security tools such as digital certificates, training, etc.
- Establish a single point of contact for local health jurisdictions to communicate changes in individuals approved access.
- Coordinate an approach for maintaining a tracking system and providing routine reports to local health jurisdiction leadership that includes 1) who has been granted access and which type of rights to what; 2) who has signed the necessary paperwork such as security and confidentiality statements and data-sharing agreements; 3) who has been trained in what and who is due for training; and 2) when each digital certificates expires or needs to be renewed.